

### **REMARKS**

This amendment is responsive to the Office Action dated June 16, 2004. No amendments have been made by way of this communication. Claims 1-22 remain pending.

#### **Claim Rejection Under 35 U.S.C. § 103**

In the Office Action, the Examiner rejected claims 1, 3, 5, 6, 7, 8, and 13 under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. (U.S. Pub. No. US 2002/0073042 A1) in view of DeLaHuerge (U.S. 6,408,330 B1). The Examiner further rejected claims 2, 4, 9, 10, 11, 12, 14-22 under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. in view of DeLaHuerge (U.S. 6,408,330 B1) and further in view of Gainsboro et al (U.S. Pub. No. US 2001/0036821 A1), Blumenau et al. (U.S. Pub. No. US 2001/0020254 A1) and Atsmon et al. (US 6,607,136).

Applicant respectfully traverses the rejection. The applied references fail to disclose or suggest the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

As described in the present application, embodiments of a lightweight, wearable personal digital identifier device provide a high level of security by internally generating a master biometric template and private and public key pairs. Further, the personal digital identifier is configured to prevent transmission of the private key or the master biometric template from the device.

For example, the present application states that the personal digital identifier itself "includes a cryptographic software component which manages the creation of one or more public/private key pairs within the PDI 10 and all subsequent processing on the PDI 10 involving encrypting and decrypting messages."<sup>1</sup> As another example, the present application states that

*Using its microprocessor(s) 20 the PDI device itself generates and internally stores the user's biometric template and one or more public and private keys.<sup>2</sup>*

The fact that the master template for the biometric and the private key are both generated internally and not transferred to or from the mobile personal identifier device provides an

---

<sup>1</sup> Page 10, lines 16-20.

<sup>2</sup> Page 12, lines 25-30 (emphasis added).

increased level of security over conventional devices. None of the references cited by the Examiner teach or suggest these features.

With reference to independent claims 1 and 9, the applied references lack any teaching that would have suggested, among other features, a personal digital identifier device comprising a processor generating a private key held by the personal digital identifier device. The applied references also fail to teach or suggest a personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key, as required by claims 1 and 9.

With respect to independent claim 17, among other features, the applied references lack any teaching that would have suggested a method comprising, within said portable personal digital identifier device: receiving an input biometric of said user, producing a digital representation thereof, deriving from said digital representation a master template, securely maintaining said master template in storage, generating and securely maintaining in said storage a private key.

Maritzen et al., describes an electronic "privacy card" for verifying a user connecting to an electronic commerce system. Specifically, the "privacy card" maintains the privacy of the user while enabling the user to perform transactions. Information from the privacy card is provided to a "transaction privacy clearing house" (TPCH) to indicate approval of the transaction to be performed.<sup>3</sup> Maritzen et al also describes a digital wallet that provides an interface between the privacy card and the eCommerce network.

The Examiner is correct that Maritzen describes a privacy card that includes a user authentication block for authenticating fingerprints of a user. However, neither Maritzen nor any of the other cited references describe a portable personal digital identifier device that internally generates and securely maintains a private key. Further, none of the references describe a personal digital identifier device that is configured to prevent transmission of the private key and a master biometric template from the identifier device.

To the contrary, Maritzen specifically states that the digital wallet assigns one or more private keys to the card, and that the privacy card records the keys in secure memory.<sup>4</sup> Figure 12

---

<sup>3</sup> Paragraph 47.

<sup>4</sup> Paragraph 157.

shows that the keys are provided to and subsequently stored in the privacy card. Thus, contrary to Applicant's claims, the private key associated with the privacy card of Maritzen is generated external to the privacy card, and downloaded to the privacy card.

Moreover, Figure 11 of Maritzen shows that the user's fingerprint sample is communicated from a fingerprint recognition pad to the transaction privacy clearing house associated with the network. In describing Figure 11, in paragraph 0143, Maritzen states:

*At step 1101, after filling out the transaction device registration form, the user presses the "submit form" button or other appropriate trigger mechanism. The user is prompted to touch the fingerprint recognition pad in order to provide non-repudiation data (the user is "signing" the form and verifying that the user wants to register), and is providing the fingerprint identity sample that will be stored in the transaction device by the processing facility, for example, the TPC. At step 1102 the PC software encrypts all of the information and delivers it to the TPC over a secure connection.*

Consequently, the teachings of Maritzen are directly contrary to Applicant's claims. The applied references lack any teaching that would have suggested a personal digital identifier device comprising a processor generating a private key held by the personal digital identifier device. Further, the applied references fail to teach or suggest a personal digital identifier device being configured to prevent transmission of the master template of a user's biometric and the private key generated internally by the device, as required by claims 1 and 9.

None of the references overcome these and other deficiencies and contrary teachings of Maritzen. For example, it appears that the cited portion of DeLaHuerga teaches the use of a public key to authenticate a document. Neither DeLaHuerga nor any of the other references teach or suggest these and other features of Applicant's independent claims.

Dependent claims 2-8, 10-16, and 17-22 are allowable for at least the reasons set forth above. With respect to claim 22, Applicant particularly points out that none of the references remotely suggest a policy manager component that directs that the screen of a workstation be blanked out when a new personal digital identifier device moves to a location within said envelope until such time as the user registered to said personal digital identifier device is biometrically identified. In rejecting claim 22, the Examiner cites column 35, lines 35-50 of DeLaHuerga. However, in this portion, DeLaHuerga appears to describe a process for

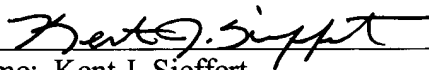
associating patient records with a patient's identification. DeLaHuerga describes closing a session when the personal device is not associated with a patient record selected to be downloaded. Nowhere does DeLaHuerga describe blanking a screen of a workstation when a new personal digital identifier devices moves to a location within an envelope around the workstation until the user is biometrically identified, as required by claim 22.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

### CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:  
October 18, 2004  
SHUMAKER & SIEFFERT, P.A.  
8425 Seasons Parkway, Suite 105  
St. Paul, Minnesota 55125  
Telephone: 651.735.1100  
Facsimile: 651.735.1102

By:  
  
Name: Kent J. Sieffert  
Reg. No.: 41,312